

# Experimental Verification of Multipartite Entanglement in Quantum Networks

W. McCutcheon,<sup>1</sup> A. Pappa,<sup>2,\*</sup> B. A. Bell,<sup>1</sup> A. McMillan,<sup>1</sup> A. Chailloux,<sup>3</sup> T. Lawson,<sup>4</sup>  
M. Mafu,<sup>5</sup> D. Markham,<sup>4</sup> E. Diamanti,<sup>4</sup> I. Kerenidis,<sup>6,7</sup> J. G. Rarity,<sup>1</sup> and M. S. Tame<sup>8,9,†</sup>

<sup>1</sup>*Quantum Engineering Technology Laboratory, Department of Electrical and Electronic Engineering,  
University of Bristol, Woodland Road, Bristol, BS8 1UB, UK*

<sup>2</sup>*School of Informatics, University of Edinburgh, Edinburgh EH89AB, UK*

<sup>3</sup>*INRIA, Paris Rocquencourt, SECRET Project Team, Paris, France*

<sup>4</sup>*LTCI, CNRS, Telecom ParisTech, Université Paris-Saclay, 75013 Paris, France*

<sup>5</sup>*Department of Physics and Astronomy, Botswana International University of Science and Technology, P/Bag 16 Palapye, Botswana*

<sup>6</sup>*CNRS IRIF, Université Paris 7, Paris 75013, France*

<sup>7</sup>*Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543, Singapore*

<sup>8</sup>*School of Chemistry and Physics, University of KwaZulu-Natal, Durban 4001, South Africa*

<sup>9</sup>*National Institute for Theoretical Physics, University of KwaZulu-Natal, Durban 4001, South Africa*

(Dated: November 16, 2016)

Multipartite entangled states are a fundamental resource for a wide range of quantum information processing tasks. In particular, in quantum networks it is essential for the parties involved to be able to verify if entanglement is present before they carry out a given distributed task. Here we design and experimentally demonstrate a protocol that allows any party in a network to check if a source is distributing a genuinely multipartite entangled state, even in the presence of untrusted parties. The protocol remains secure against dishonest behaviour of the source and other parties, including the use of system imperfections to their advantage. We demonstrate the verification protocol in a three- and four-party setting using polarization-entangled photons, highlighting its potential for realistic photonic quantum communication and networking applications.

## INTRODUCTION

Entanglement plays a key role in the study and development of quantum information theory and is a vital component in quantum networks [1–5]. The advantage provided by entangled states can be observed, for example, when the quantum correlations of the  $n$ -party Greenberger-Horne-Zeilinger (GHZ) state [6] are used to win a nonlocal game with probability 1, while any classical local theory can win the game with probability at most  $3/4$  (see Ref. [7]). In a more general setting, multipartite entangled states allow the parties in a network to perform distributed tasks that outperform their classical counterparts [8], to delegate quantum computation to untrusted servers [9], or to compute through the measurement-based quantum computation model [10]. It is therefore vital for parties in a quantum network to be able to verify that a state is entangled, especially in the presence of untrusted parties and by performing only local operations and classical communication.

A protocol for verifying that an untrusted source creates and shares the  $n$ -qubit multipartite entangled GHZ state,  $|GHZ_n\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes n} + |1\rangle^{\otimes n})$ , with  $n$  parties has recently been proposed [11]. In the verification protocol, the goal of the honest parties is to determine how close the state they share is to the ideal GHZ state and verify whether or not it contains genuine multipartite entanglement (GME) – entanglement that can only exist if all qubits were involved in the creation of the state [1]. On the other hand, any number of dishonest parties that may collaborate with the untrusted source are trying to ‘cheat’ by convincing the honest parties that the state they share is close to the ideal GHZ state and contains GME when this may not be the case. Verifying GME in mul-

tipartite GHZ states in this way is relevant to a wide variety of protocols in distributed quantum computation and quantum communication. While distributed quantum computation is at an early stage of development experimentally [12–14], many schemes for using multipartite GHZ states in distributed quantum communication have already been demonstrated, including quantum secret sharing [15], open-destination teleportation [16] and multiparty quantum key distribution [17, 18]. This makes the entanglement verification protocol relevant for distributed quantum communication with present technology.

In order for a quantum protocol to be practical, however, it must take into account system imperfections, including loss and noise, throughout the protocol (generation, transmission and detection of the quantum state). In previous work [11], it was shown that by using a suitable protocol, the closeness of a shared resource state to a GHZ state and the presence of GME can be verified in a distributed way between untrusted parties under perfect experimental conditions. However, the protocol is not tolerant to arbitrary loss and in fact it cannot be used for a loss rate that exceeds 50%.

In this work, we design and experimentally demonstrate a protocol that outperforms the original one in Ref. [11]. We examine quantitatively how a dishonest party can use system imperfections to boost their chances of cheating and show our protocol defends against such tactics. We demonstrate both the original and new protocols using a source of polarization-entangled photons, which produces three- and four-party GHZ states, and examine the performance of the protocols under realistic experimental conditions. Our results are perfectly adapted to photonic quantum networks and can be used to reliably verify multipartite entanglement in a real-world quantum communication setting. In order to achieve verification of a state in an untrusted setting, the protocols exploit the capabil-



whether or not it contains GME. The protocol to do this is as follows: First, the Verifier generates random angles  $\theta_j \in [0, \pi)$  for all parties including themselves ( $j \in [n]$ ), such that  $\sum_j \theta_j$  is a multiple of  $\pi$ . The angles are then sent out to all the parties in the network. When party  $j$  receives their angle from the Verifier they measure in the basis  $\{|+\theta_j\rangle, |-\theta_j\rangle\} = \{\frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta_j}|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - e^{i\theta_j}|1\rangle)\}$  and send the outcome  $Y_j = \{0, 1\}$  to the Verifier. A flow diagram of the protocol is shown in Fig. 1a, where the order in which the angles are sent out and outcomes returned is irrelevant and it is assumed that the Verifier and each of the parties share a secure private channel for the communication. This can be achieved by using either a one-time pad or quantum key distribution [3], making the communication secure even in the presence of a quantum computer. The state passes the test when the following condition is satisfied: if the sum of the randomly chosen angles is an even multiple of  $\pi$ , there must be an even number of 1 outcomes for  $Y_j$ , and if the sum is an odd multiple of  $\pi$ , there must be an odd number of 1 outcomes for  $Y_j$ . We can write this condition as

$$\bigoplus_j Y_j = \frac{1}{\pi} \sum_j \theta_j \pmod{2}. \quad (1)$$

For an ideal  $n$ -qubit GHZ state, the test succeeds with probability 1 (see Supplementary Note 1). Moreover, it can be shown that the fidelity  $F(\rho) = \langle \text{GHZ}_n | \rho | \text{GHZ}_n \rangle$  of a shared state  $\rho$  with respect to an ideal GHZ state can be lower bounded by a function of the probability of the state passing the test,  $P(\rho)$ . If we first suppose that all  $n$  parties are honest, then  $F(\rho) \geq 2P(\rho) - 1$  (see Supplementary Note 1). Furthermore, we can say that GME is present for a state  $\rho$  when  $F(\rho) > 1/2$  with respect to an ideal GHZ state [23] and therefore GME can be verified when the pass probability is  $P(\rho) > 3/4$ . This verification protocol, that we will call the ‘ $\theta$ -protocol’, is a generalisation of the protocol in Ref. [11], called the ‘XY-protocol’, where the angles  $\theta_j$  are fixed as either 0 or  $\pi/2$ , corresponding to measurements in the Pauli  $X$  or  $Y$  basis. In the honest case and under ideal conditions, the lower bound for the fidelity is the same in both protocols.

When the Verifier runs the test in the presence of  $n - k$  dishonest parties, the dishonest parties can always collaborate and apply a local or joint operation  $U$  to their part of the state. This encompasses the different ways in which the dishonest parties may try to cheat in the most general setting. Hence, we look at a fidelity measure given by  $F'(\rho) = \max_U F((\mathbb{I}_k \otimes U_{n-k})\rho(\mathbb{I}_k \otimes U_{n-k}^\dagger))$ , and lower bound it by the pass probability as  $F'(\rho) \geq 4P(\rho) - 3$  for both the  $\theta$  and XY protocols (see Supplementary Note 1). This gives directly a bound of  $P(\rho) > 7/8 = 0.875$  to observe GME. However, by concentrating on attacks for the case  $F'(\rho) = 1/2$ , tighter analysis can be performed (see Supplementary Note 1), where the GME bound can be shown to be  $P(\rho) \geq 1/2 + 1/\pi \approx 0.818$  for the  $\theta$ -protocol and  $P(\rho) \geq \cos^2(\pi/8) \approx 0.854$  for the XY protocol. The  $\theta$ -protocol is more sensitive to detecting cheating and hence can be used to verify GME more broadly in realistic

implementations where the resources are not ideal.

The above bounds do not account for loss. To analyse cheating strategies which take advantage of loss we must allow the dishonest parties (which have potentially perfect control of the source and their equipment) to choose to declare ‘loss’ at any point. In particular they may do this when they are asked to make measurements that would reduce the probability of success, making the round invalid, which can skew the statistics in favour of passing to the advantage of the dishonest parties. This may change the fidelity and GME bounds above. We address this to find GME bounds in the case of loss in our photonic realization.

## Experimental setup

The optical setup used to perform the verification protocols is shown in Fig. 1b. The source of GHZ states consists of two micro-structured photonic crystal fibers (PCFs), each of which produces a photon pair by spontaneous four-wave mixing, with the signal wavelength at 623 nm and the idler at 871 nm (see Supplementary Note 2). To generate entangled pairs of photons, each fibre loop is placed in a Sagnac configuration, where it is pumped in both directions. When the pump pulse entering the Sagnac loop is in diagonal polarisation, conditional on a single pair being generated by the pump laser the state exiting the polarising beamsplitter (PBS) of the loop is in the Bell state  $\frac{1}{\sqrt{2}}(|H\rangle_s |H\rangle_i + |V\rangle_s |V\rangle_i)$ , with  $s$  and  $i$  indicating the signal and idler photons, respectively [24, 25]. The signal and idler photons of each source are then separated into individual spatial modes by dichroic mirrors, after which the two signal photons are overlapped at a PBS that performs a parity check, or ‘fusion’ operation [26, 27]. We postselect with 50% probability the detection outcomes in which one signal photon emerges from each output mode of the PBS which projects the state onto the four-photon GHZ state

$$\frac{1}{\sqrt{2}} (|H\rangle_{i_1} |H\rangle_{s_1} |H\rangle_{s_2} |H\rangle_{i_2} + |V\rangle_{i_1} |V\rangle_{s_1} |V\rangle_{s_2} |V\rangle_{i_2}). \quad (2)$$

All four photons are then coupled into single-mode fibres, which take them to measurement stages representing the parties in the network. With appropriate angle choices of the wave plates included in these stages any projective measurement can be made by the parties on the polarisation state of their photon [28]. In our experiment the successful generation of the state is conditional on the detection of four photons in separate modes, *i.e.* postselected. In principle it is possible to move beyond postselection in our setup, where the GHZ states are generated deterministically. This can be achieved by the addition of a quantum non-demolition (QND) measurement of the photon number in the modes after the fusion operation. While technically challenging, QND measurements are possible for photons, for instance as theoretically shown [29, 30] and experimentally demonstrated [31]. By using postselection we are able to give a proof-of-principle demonstration of the

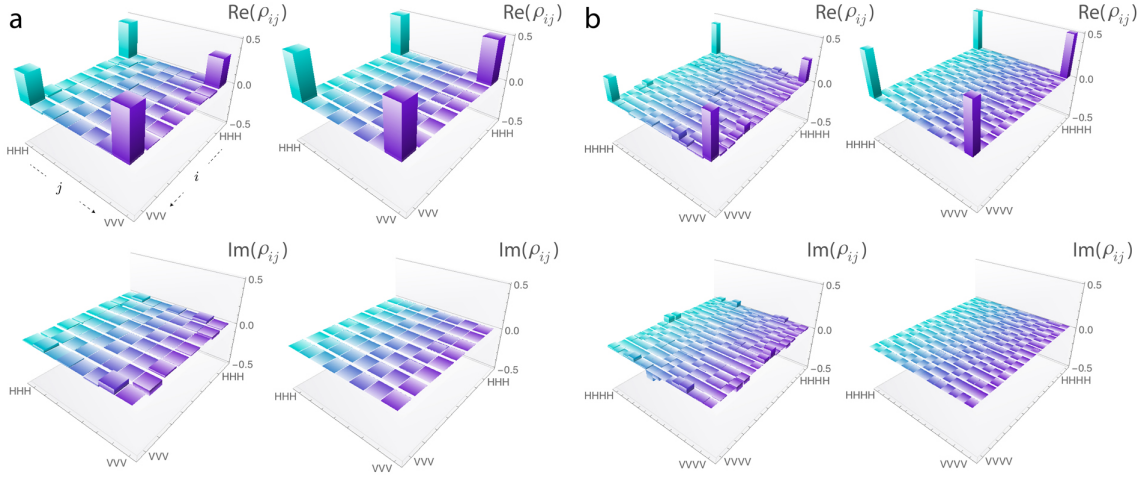


FIG. 2: Tomographic reconstruction of the three- and four-photon GHZ states used in the protocols. **a**, Three-photon GHZ state (left column) and ideal case (right column). **b**, Four-photon GHZ state (left column) and ideal case (right column). Top row corresponds to the real parts and bottom row corresponds to the imaginary parts. The density matrix elements are given by  $\rho_{ij} = \langle i | \rho_{exp} | j \rangle$ , where  $\rho_{exp}$  is the reconstructed experimental density matrix.

protocols and gain important information about their performance in such a scenario, including the impact of loss.

In our experiments we use both a three- and a four-photon GHZ state. The generation of the three-photon state requires only a slight modification to the setup, with one of the PCFs pumped in just one direction to generate unentangled pairs (see Supplementary Note 2). Before carrying out the verification protocols we first characterise our experimental GHZ states by performing quantum state tomography [28]. The resulting density matrices for the three- and four-photon GHZ states are shown in Fig. 2 and have corresponding fidelities  $F_{GHZ_3} = 0.80 \pm 0.01$  and  $F_{GHZ_4} = 0.70 \pm 0.01$  with respect to the ideal states. These fidelities compare well with other recent experiments using photons (see Table 1) and are limited mainly by dephasing from the fusion operation [26] and higher-order emission (see Supplementary Note 2). The errors have been calculated using maximum likelihood estimation and a Monte Carlo method with Poissonian noise on the count statistics, which is the dominant source of error in our photonic experiment [28].

3-photon GHZ Fidelity	4-photon GHZ Fidelity
$F = 0.80 \pm 0.01$ , this work	$F = 0.70 \pm 0.01$ , this work
$F = 0.768 \pm 0.015$ [35]	$F = 0.840 \pm 0.007$ [33]
$F = 0.74 \pm 0.01$ [36]	$F = 0.66 \pm 0.01$ [27]
$F = 0.811 \pm 0.002$ [37]	$F = 0.833 \pm 0.004$ [34]
$F = 0.93 \pm 0.01$ [38]	

TABLE I: Comparison of GHZ fidelities. The table shows the fidelity of recent three-photon and four-photon GHZ states from other experiments, and includes the fidelities from this work (top row).

### Entanglement verification

To demonstrate the verification of multipartite entanglement we use the polarisation degree of freedom of the photons generated in our optical setup. The computational basis states sent out to the parties are therefore defined as  $|0\rangle = |H\rangle$  and  $|1\rangle = |V\rangle$  for a given photon. Furthermore, the verification protocol relies on a randomly selected set of angles being distributed by the Verifier for each state being tested. To ensure dishonest parties have no prior knowledge, the set of angles is changed after every detection of a copy of the state, *i.e.* we perform *single-shot* measurements in our experiment. To achieve this, we use automated wave-plate rotators to change the measurement basis defined by the randomised angles for each state. The rotators are controlled by a computer with access to the incoming coincidence data. This approach is needed to provide a faithful demonstration of the protocol and is technologically more advanced than the usual method used in photonic quantum information experiments, where many detections are accumulated over a fixed integration time for a given measurement basis and properties then inferred from the ensemble of states. We now analyse the performance of the XY and  $\theta$  verification protocols for the three- and four-party GHZ states.

*1. Verification of three-party GHZ* – The XY verification protocol was initially carried out using the three-photon GHZ state, with all parties behaving honestly. The first two angles  $\theta_j$  were randomly chosen to be either 0 or  $\pi/2$ , with the third angle representing the Verifier being decided so that  $\sum_j \theta_j$  is a multiple of  $\pi$ . After repeating the protocol on 6000 copies of the state, the pass probability was found to be  $0.838 \pm 0.005$ . Similarly, the  $\theta$ -protocol was carried out, with the first two angles chosen uniformly at random from the continuous range  $[0, \pi)$ . After 6000 copies of the state were prepared and mea-

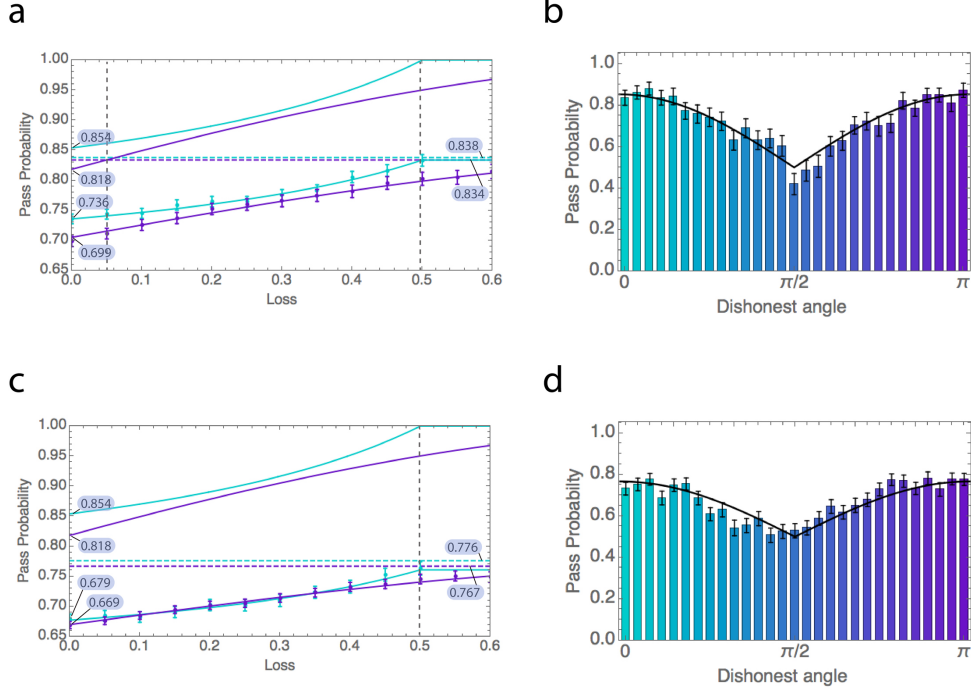


FIG. 3: Pass probabilities as a function of loss for one dishonest party in a three- and four-party setting. Panels **a** and **b** correspond to the three-party setting, and panels **c** and **d** correspond to the four-party setting. The upper curves in panels **a** and **c** show the ideal theoretical case for the GME bound for the  $\theta$ -protocol (purple curve) and a cheating strategy for the XY-protocol (turquoise curve) that always performs better. Note that the XY-protocol cannot be used here for verification as the non-GME dishonest value is always above the honest value. The lower solid curves in panels **a** and **c** correspond to the experimental results obtained for the three- and four-photon GHZ state, respectively. In both panels, the dashed lines correspond to the honest experimental values when there is no loss (turquoise for the XY-protocol and purple for the  $\theta$ -protocol). Panels **a** and **c** clearly show that the  $\theta$ -protocol can tolerate loss  $\geq 0.5$  in the ideal case. Panels **b** and **d** show the optimal pass probability that the dishonest party can obtain when running the  $\theta$ -protocol with no loss, for a given dishonest angle  $\theta$ , for the three-party and four-party case, respectively. In all plots the curves are a best fit to the data. All error bars represent the standard deviation and are calculated using a Monte Carlo method with Poissonian noise on the count statistics [28].

sured, the pass probability was found to be  $0.834 \pm 0.005$ .

Using the relation between the fidelity and the pass probability,  $F(\rho) \geq 2P(\rho) - 1$ , the Verifier can conclude that the fidelity with respect to an ideal GHZ state is at least  $0.676 \pm 0.010$  for the XY-protocol and at least  $0.668 \pm 0.010$  for the  $\theta$ -protocol. These values are consistent with the value obtained using state tomography. Despite the non-ideal experimental resource, the lower bound on the fidelity is clearly above  $1/2$  and therefore sufficient for the Verifier to verify GME in this all honest case.

More importantly, the  $\theta$ -protocol enables the Verifier to verify GME even when they do not trust all of the parties. Indeed, the experimental value of the pass probability,  $0.834$ , exceeds by more than three standard deviations the GME bound of  $0.818$  for the dishonest case. We remark that for verifying GME in these conditions we crucially used the fact that our three-qubit GHZ state has very high fidelity and that the  $\theta$ -protocol has improved tolerance to noise. In fact, the Verifier is not able to verify GME using the XY-protocol, since the experimental value of  $0.838$  does not exceed the GME bound of  $0.854$ .

## 2. Verification of three-party GHZ with loss (theory) – We

now investigate the impact of loss on the performance of the verification protocols. In this setting, the Verifier is willing to accept up to a certain loss rate from each party. When a party declares loss, the specific run of the protocol is aborted and the Verifier moves on to testing the next copy of the resource state. A dishonest party, who may not have the maximum allowed loss rate in their system, or may even have no loss at all, can increase the overall pass probability of the state by declaring loss whenever the probability to pass a specific measurement request from the Verifier is low.

For example, a non-GME state can have pass probability 1 for the XY-protocol when the allowed loss rate is 50%. In this case, the source can share a state of the form  $\frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle) \otimes |+\rangle$ , where the third qubit is sent to a dishonest party. Then, when the latter is asked to measure in the Pauli X basis, he always answers correctly, while when asked to measure in the Pauli Y basis he declares loss. Of course, such a strategy would alert the Verifier that the party is cheating, since he is always declaring loss when asked to measure in the Y basis, while when asked to measure in the X basis, he always measures the  $|+\rangle$  eigenstate. However, if the source and the dishonest party are collaborating, and the source is able to create

and share any Bell pair with the two honest parties, then the test can be passed each time without the cheating detected. The dishonest strategy would go as follows: the source sends randomly one of the four states  $\{\frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle), \frac{1}{\sqrt{2}}(|HH\rangle - |VV\rangle), \frac{1}{\sqrt{2}}(|HH\rangle + i|VV\rangle), \frac{1}{\sqrt{2}}(|HH\rangle - i|VV\rangle)\}$  and tells the dishonest party which one was sent, so that the latter can coordinate his actions. For the first state he replies 0 only for the  $X$  basis, for the second state he replies 1 only for the  $X$  basis, for the third he replies 1 only for the  $Y$  basis and for the fourth he replies 0 only for the  $Y$  basis.

More generally, we can analytically find the GME bound as a function of the loss rate for both protocols and describe optimal cheating strategies to achieve these bounds with non-GME states. The optimal cheating strategy for the  $XY$ -protocol consists of the source rotating the non-GME state that is sent to the honest parties in a specific way depending on the amount of loss allowed, and informing the dishonest party about the rotation. For zero loss, the optimal state is the  $\pi/4$ -rotated Bell pair  $\frac{1}{\sqrt{2}}(|HH\rangle + e^{i\frac{\pi}{4}}|VV\rangle)$ , while for 50% loss, the optimal state is the Bell pair  $\frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle)$ . For any loss,  $\lambda$ , in between, the dishonest strategy is a probabilistic mixture of these two strategies; it consists of sending the Bell pair with probability  $2\lambda$  (and discarding the rounds in which the dishonest party is asked to measure  $Y$ ), and the  $\pi/4$ -rotated Bell pair with probability  $1 - 2\lambda$ . In both, the strategy mentioned in the previous paragraph for avoiding detection of the dishonest party's cheating is required. On the other hand, the optimal strategy for the  $\theta$ -protocol is having the source send a rotated Bell pair with the dishonest party declaring loss for the angles that have the lowest pass probability (see Supplementary Note 1).

The upper bounds of the pass probability for the optimal cheating strategies using a non-GME state are shown as the solid turquoise and purple upper curves in Fig. 3, for the  $XY$  and  $\theta$ -protocol respectively. Specifically for the case of no loss, we recover the GME bounds of 0.854 and 0.818 for the  $XY$ - and  $\theta$ -protocol, respectively. The GME bound for the  $XY$ -protocol reaches 1 for 50% loss, while the GME bound for the  $\theta$  protocol reaches 1 only at 100% loss.

**3. Verification of three-party GHZ with loss (experiment)** – In Fig. 3a one can see the experimental value of  $0.834 \pm 0.005$  when there is no loss for the  $\theta$ -protocol enables the Verifier to verify GME in the presence of up to  $\sim 5\%$  loss – once the loss increases past 5%, the Verifier can no longer guarantee the shared experimental state has GME. Again, this loss tolerance is only possible due to the high fidelity of our three-party GHZ state and the fact that our  $\theta$ -protocol has a better behaviour with respect to loss. The tolerance to loss can be further improved using experimental states with higher fidelities. However, it is interesting to note that 5% loss corresponds to  $\sim 1$  km of optical fibre, which already makes the protocol relevant to a quantum network within a small area, such as a city or government facility, where a number of quantum communication protocols could be carried out over the network, such as, for instance quantum secret sharing [15], telecloning [32]

and open destination teleportation [16].

**4. Implementation of dishonest strategies for three-party GHZ** – In order to maximise the pass probabilities of the protocols using a non-GME state, the source needs to appropriately rotate the state that is sent to the honest parties depending on the amount of loss allowed. We implemented this strategy for a single dishonest party by using a complementary method, where the source creates a three-qubit GHZ state and gets the dishonest party to perform a projective measurement that creates the necessary rotated non-GME state between the honest parties. This strategy was performed experimentally for both protocols on 3000 copies of the three-qubit GHZ state. Since in our experiment the GHZ states are created by postselection, the loss corresponds to the allowed percentage of tests in which the dishonest party can claim they lost their qubit during transmission of the corresponding photon from the source.

The pass probabilities are shown as a function of loss by the solid turquoise and purple lower curves in Fig. 3a. They show the same trend as the previous curves but are shifted lower due to the non-ideal experimental state. For the no loss case, we obtain a pass probability of  $0.736 \pm 0.008$  for the  $XY$ -protocol. For the  $\theta$ -protocol, the pass probability depends on the dishonest party's measurement request  $\theta$ : for no loss, the experimental results are shown in Fig. 3b, from which we obtain an average pass probability of  $0.699 \pm 0.009$ . When loss is included the dishonest party's cheating strategy leads to a higher pass probability, since the dishonest party claims loss when the angle given to him by the Verifier is close to  $\pi/2$ , corresponding to the minimum pass probability shown in Fig. 3b. Similar to the discussion in the example of the  $XY$ -protocol, the source collaborates with the dishonest party and applies a rotation to the shared state, so that the declared lost angles appear uniform and not always around  $\pi/2$ .

**5. Verification of four-party GHZ** – To check the performance of the protocols for a higher number of parties, the verification tests were carried out using the four-photon GHZ state generated in our experiment, now with three angles chosen randomly, and the fourth depending on the condition that  $\sum_j \theta_j$  is a multiple of  $\pi$ . Again, we start with the all honest case where any of the parties may be the Verifier. For the  $XY$ -protocol, with all  $\theta_j$  equal to 0 or  $\pi/2$ , the pass probability for 6000 copies of the state was found to be  $0.776 \pm 0.005$ . For the  $\theta$ -protocol, using 6000 copies, the pass probability was found to be  $0.767 \pm 0.005$ .

As in the three-party case, the Verifier can conclude that the fidelity with respect to an ideal GHZ state is at least  $0.552 \pm 0.010$  for the  $XY$ -protocol and at least  $0.534 \pm 0.010$  for the  $\theta$ -protocol, therefore just sufficient for the Verifier to verify that GME is present in the state. Again, the high fidelity of our experimental state is crucial for this result. Nevertheless, none of the two protocols can confirm GME in the presence of dishonest parties since the pass probabilities are below the GME bounds of 0.854 and 0.818, respectively.

**6. Implementation of dishonest strategies for four-party GHZ** – The dishonest strategies that are used to implement



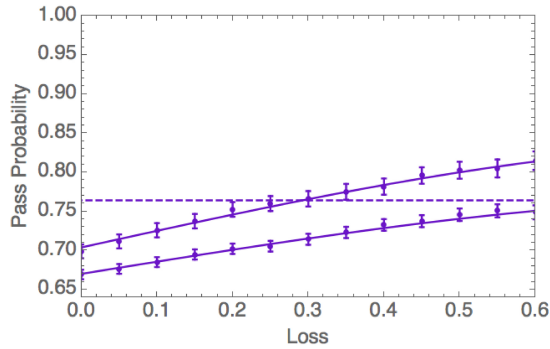


FIG. 4: Impact of noise and loss on the pass probability of the  $\theta$ -verification protocol in a four-party setting. The lower curve corresponds to a biseparable state (four-qubit GHZ state with a projective measurement on the dishonest qubit) and the upper curve corresponds to a biseparable state (three-qubit GHZ state and an unentangled qubit for the dishonest player) that has less noise. The dashed line corresponds to the honest case. All error bars represent the standard deviation and are calculated using a Monte Carlo method with Poissonian noise on the count statistics [28].

the two verification protocols for different amounts of loss are the same as in the three-party case. However, we proceed in two different ways for a single dishonest party. First, we have the source create our non-ideal four-qubit GHZ state and then allow the dishonest party to perform the dishonest projective measurement in order to create a non-GME state. When there is no loss we obtain a pass probability of  $0.679 \pm 0.008$  for the XY-protocol and  $0.669 \pm 0.008$  for the  $\theta$ -protocol (averaged over the dishonest angle  $\theta$ , as shown in the histogram of Fig. 3d). When loss is included, the pass probabilities of both the XY- and  $\theta$ -protocols increase, as the dishonest party uses the loss to their advantage (see Fig. 3c). A second way to implement the dishonest strategy is to have the source create the non-ideal three-qubit GHZ state for the honest parties and the dishonest party hold an unentangled photon. This results in a four-party non-GME state with reduced noise – as the dephasing from the entangled pair of the second PCF is no longer present [26]. We perform the  $\theta$ -protocol with this better quality resource state and see that the pass probability increases from  $0.669 \pm 0.005$  to  $0.698 \pm 0.008$  for the no loss case and remains higher when loss is included (see Fig. 4). Note that despite the second strategy having higher pass probabilities, these are still below the GME bound shown in Fig. 3c (upper purple curve).

The comparison of the two strategies shows that the projection method is not necessarily optimal for the dishonest party due to phase noise in the experimental state. Note also that as the pass probability of the experimental state in the honest case (dotted purple line in Fig. 3c) is below the GME bound, the Verifier is not able to verify GME for this four-party setting for any amount of loss. Verification of GME is achieved in our experiment only in the three-party setting. However, four-party verification could be achieved using experimental states with higher fidelities, and even with our non-ideal three-

party GHZ state we have been able to provide the first proof-of-principle demonstration of our GME verification protocol.

## DISCUSSION

The results we have presented are situated in a realistic context of distributed communication over photonic quantum networks: we have shown that it is possible for a party in such a network to verify the presence of genuine multipartite entanglement in a shared resource, even when some of the parties are not trusted, including the source of the resource itself. This distrustful setting sets particularly stringent conditions on what can be shown in practice. With our state-of-the-art optical setup that produces high-fidelity three- and four-photon GHZ states, we were able to show, for the three-party case, that this verification process is possible using a carefully constructed protocol, for up to 5% loss, under the most strict security conditions. Clearly, the loss tolerance of the system can be further improved by using states with even higher fidelities. This would also enable the implementation of the verification protocols for a larger number of qubits.

It is important to remark that our verification protocols go beyond merely detecting entanglement; they also link the outcome of the verification tests to the state that is actually used by the honest parties of the network with respect to their ideal target state. This is non trivial and of great importance in a realistic setting where such resources are subsequently used by the parties in distributed computation and communication applications executed over the network. Such applications may also require multipartite entangled states other than the GHZ states studied in this work. We expect that our verification protocols should indeed be applicable to other types of useful states such as, for instance, stabiliser states.

## ACKNOWLEDGMENTS

This work was supported by the UK's Engineering and Physical Sciences Research Council, ERC grants 247462 QUOWSS and QCC, EU FP7 grant 600838 QWAD, the Ville de Paris Emergences project CiQWii, the ANR project COMB, the Ile-de-France Region project QUIN and the South African National Research Foundation.

\* Electronic address: annapappa@gmail.com

† Electronic address: markstame@gmail.com

- [1] R. Horodecki, P. Horodecki, M. Horodecki, K. Horodecki, Quantum Entanglement, Rev. Mod. Phys. **81**, 865 (2009).
- [2] H. J. Kimble, The quantum internet, Nature **453**, 1023-1030 (2008).
- [3] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, M. Peev, The practical security of quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).

- [4] G. Chiribella, G. M. D'Ariano, P. Perinotti, Theoretical framework for quantum networks, *Phys. Rev. A* **80**, 022339 (2009).
- [5] S. Perseguers, G. J. Lapeyre Jr, D. Cavalcanti, M. Lewenstein, A. Acin, Distribution of entanglement in large-scale quantum networks, *Rep. Prog. Phys.* **76** 096001 (2013).
- [6] D. M. Greenberger, M. A. Horne, A. Zeilinger, Going beyond Bell's theorem, in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, M. Kafatos (Ed.), Kluwer, Dordrecht, 1989, pp. 69–72.
- [7] N. D. Mermin, Extreme quantum entanglement in a superposition of macroscopically distinct states, *Phys. Rev. Lett.* **65**, 1838 (1990).
- [8] H. Buhrman, R. Cleve, S. Massar, R. de Wolf, Nonlocality and communication complexity, *Rev. Mod. Phys.* **82**, 665 (2010).
- [9] A. Broadbent, J. Fitzsimons, E. Kashefi, Universal blind quantum computation, in *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS)* 2009, pp. 517–526.
- [10] R. Raussendorf, H. J. Briegel, A one-way quantum computer, *Phys. Rev. Lett.* **86**, 5188 (2001).
- [11] A. Pappa, A. Chailloux, S. Wehner, E. Diamanti, I. Kerenidis, Multipartite Entanglement Verification Resistant against Dishonest Parties. *Phys. Rev. Lett.* **108**, 260502 (2012).
- [12] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger and P. Walther, Experimental Demonstration of Blind Quantum Computing, *Science* **335**, 303-308 (2012).
- [13] S. Barz, J. F. Fitzsimons, E. Kashefi and P. Walther, Experimental verification of quantum computation, *Nat. Phys.* **9**, 727-731 (2013).
- [14] C. Greganti, M.-C. Roehsner, S. Barz, T. Morimae and P. Walther, Demonstration of measurement-only blind quantum computing, *New J. Phys.* **18**, 013020 (2016).
- [15] W. Tittel, H. Zbinden and N. Gisin, Experimental demonstration of quantum secret sharing, *Phys. Rev. A* **63**, 042301 (2001).
- [16] Z. Zhao, Y.-A. Chen, A.-N. Zhang, T. Yang, H. J. Briegel and J.-W. Pan, Experimental demonstration of five-photon entanglement and open-destination teleportation, *Nature* **430**, 54-58 (2004).
- [17] Y.-A. Chen, A.-N. Zhang, Z. Zhao, X.-Q. Zhou, C.-Y. Lu, C.-Z. Peng, T. Yang and J.-W. Pan, Experimental Quantum Secret Sharing and Third-Man Quantum Cryptography, *Phys. Rev. Lett.* **95**, 200502 (2005).
- [18] R. B. A. Adamson, B. Fortescue, H. K. Lo and A. M. Steinberg, Experimental implementation of a three-party quantum key distribution protocol, *IEEE Conf. Las. Elec. Opt.*, 1-2 (2006)
- [19] D. Mayers and A. Yao, Self testing quantum apparatus, *QIC*, **4**, 273-286 (2004).
- [20] K. F. Pal, T. Vertesi and M. Navascues, Device-independent tomography of multipartite quantum states, *Phys. Rev. A* **90**, 042340 (2014).
- [21] Matthew McKague, Self-Testing Graph States, *Proceedings of Theory of Quantum Computation, Communication, and Cryptography* 2011, Vol 6745, pp 104-120, Springer.
- [22] D. Cavalcanti, P. Skrzypczyk, G. H. Aguilar, R. V. Nery, P. H. Souto Ribeiro, S. P. Walborn, Detection of entanglement in asymmetric quantum networks and multipartite quantum steering. *Nature Communications* **6**, 7941 (2015).
- [23] G. Toth, O. Guehne, Detecting Genuine Multipartite Entanglement with Two Local Measurements, *Phys. Rev. Lett.* **94**, 060501 (2005).
- [24] M. Halder, J. Fulconis, B. Cerny, A. Clark, C. Xiong, W. J. Wadsworth, J. G. Rarity, Nonclassical 2-photon interference with separate intrinsically narrowband fibre sources, *Optics Express* **17**, 4670-4676 (2009).
- [25] A. Clark, B. Bell, J. Fulconis, M. M. Halder, B. Cerny, O. Alibart, C. Xiong, W. J. Wadsworth, J. G. Rarity, Intrinsically narrowband pair photon generation in microstructured fibres, *New J. Phys.* **13**, 065009 (2011).
- [26] B. Bell, A. Clark, M. S. Tame, M. Halder, J. Fulconis, W. Wadsworth, J. Rarity, Experimental characterization of photonic fusion using fiber sources, *New J. Phys.* **14**, 023021 (2012).
- [27] B. A. Bell, M. S. Tame, A. S. Clark, R. W. Nock, W. J. Wadsworth, J. G. Rarity, Experimental characterization of universal one-way quantum computing, *New J. Phys.* **15**, 053030 (2013).
- [28] D. F. V. James, P. G. Kwiat, W. J. Munro, A. G. White, Measurement of qubits, *Phys. Rev. A* **64**, 052312 (2001).
- [29] N. Imoto, H. A. Haus and Y. Yamamoto, Quantum nondemolition measurement of the photon number via the optical Kerr effect, *Phys. Rev. A* **32**, 2287 (1985).
- [30] Y.-F. Xiao, S. K. Ozdemir, V. Gaddam, C.-H. Dong, N. Imoto and L. Yang, Quantum nondemolition measurement of photon number via optical Kerr effect in an ultra-high-Q microtoroid cavity, *Opt. Exp.* **16**, 21462-21475 (2008).
- [31] C. Guerlin, J. Bernu, S. Deleglise, C. Sayrin, S. Gleyzes, S. Kuhr, M. Brune, J.-M. Raimond and S. Haroche, Progressive field-state collapse and quantum non-demolition photon counting, *Nature* **448**, 889-893 (2007).
- [32] M. Radmark, M. Zukowski and M. Bourennane, Experimental high fidelity six-photon entangled state for telecloning protocols, *New J. Phys.* **11**, 103016 (2009).
- [33] Z. Zhao, T. Yang, Y.-A. Chen, A.-N. Zhang, M. Zukowski and J.-W. Pan, Experimental Violation of Local Realism by Four-photon Greenberger-Horne-Zeilinger Entanglement, *Phys. Rev. Lett.*, **91** 180401 (2003).
- [34] X.-L. Wang, L.-K. Chen, W. Li, H.-L. Huang, C. Liu, C. Chen, Y.-H. Luo, Z.-E. Su, D. Wu, Z.-D. Li, H. Lu, Y. Hu, X. Jiang, C.-Z. Peng, L. Li, N.-L. Liu, Y.-A. Chen, C.-Y. Lu and J.-W. Pan, Experimental ten-photon entanglement, Preprint at <http://arxiv.org/abs/1605.08547> (2016).
- [35] K. Resch, P. Walther and A. Zeilinger, Full characterization of a three-photon GHZ state using quantum state tomography, *Phys. Rev. Lett.* **94**, 070402 (2005).
- [36] X.-Q. Zhou, C.-Y. Lu, W.-B. Gao, J. Zhang, Z.-B. Chen, T. Yang and J.-W. Pan, Greenberger-Horne-Zeilinger-type violation of local realism by mixed states, *Phys. Rev. A* **78**, 012112 (2008).
- [37] H.-X. Lu, J. Zhang, X.-Q. Wang, Y.-D. Li and C.-Y. Wang, Experimental high-intensity three-photon entangled source, *Phys. Rev. A* **78**, 033819 (2008).
- [38] R. B. Patel, J. Ho, F. Ferreyrol, T. C. Ralph and G. J. Pryde, A quantum Fredkin gate, *Sci. Adv.* **2**, e1501531 (2016).



## SUPPLEMENTARY MATERIAL

## Supplementary Figures

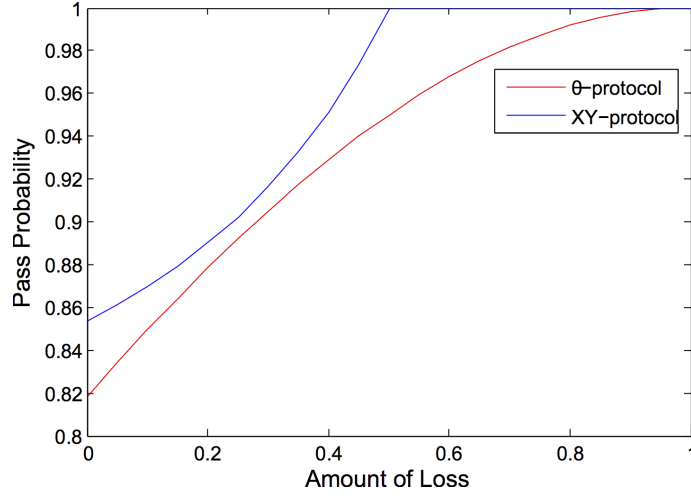


FIG. S 1: Loss tolerance of the original and new verification protocols. The  $\theta$ -protocol test performs better than the  $XY$ -protocol test and is still viable after 50% loss.

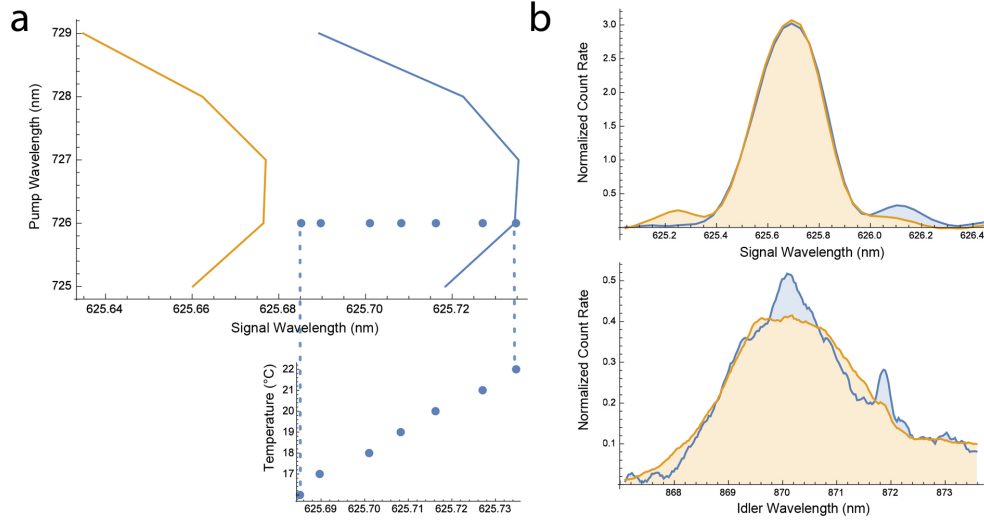


FIG. S 2: Tuning the photonic crystal fibre sources. Spectra of the microstructured photonic crystal fiber sources. **a**, Central wavelengths for source 1 (orange line) and source 2 (blue line) with varying pump wavelength. The temperature tuning of source 2 (blue points) is also shown. **b**, Spectra of signal photons (top) and idler photons (bottom) from source 1 (orange) and source 2 (blue) tuned at  $23.7^\circ\text{C}$  with a 726 nm pump.

## Supplementary Note 1

In this section we provide further details of the  $\theta$ -protocol presented in the main text (see Fig. 1). Note that the proofs for the  $XY$ -protocol follow easily as a special case with only two measurement settings.

### Correctness of the $\theta$ -protocol

Here we prove that the  $n$ -qubit GHZ state passes the verification test with probability 1. The measurements that the parties perform in the  $X$ - $Y$  plane are equivalent to rotation operators around the  $Z$  axis of the Bloch sphere:

$$R_z(\theta_j) = \begin{bmatrix} 1 & 0 \\ 0 & e^{-i\theta_j} \end{bmatrix} \quad (1)$$

followed by a measurement in the Pauli  $X$  basis. After the application of the rotation operators  $R_z(\theta_j)$  on an  $n$ -qubit GHZ state, we end up with the state  $\frac{1}{\sqrt{2}}(|0\rangle^{\otimes n} + e^{-i\Theta}|1\rangle^{\otimes n})$ , where  $\Theta = \sum_{j=1}^n \theta_j$ . When  $\Theta = 0 \pmod{2\pi}$  the shared state written in the Pauli  $X$  basis is given by a linear summation of terms with an even number of  $|-\rangle$  states for the parties. On the other hand when  $\Theta = \pi \pmod{2\pi}$  the shared state is given by a linear summation of terms with an odd number of  $|-\rangle$  states for the parties. Thus, when the parties measure their qubits in the Pauli  $X$  basis the parity of their measurements will be zero if  $\Theta = 0 \pmod{2\pi}$  and one if  $\Theta = \pi \pmod{2\pi}$ . In other words, the test will always be passed with unit probability.

### Security in the Honest Model

Now we prove a lower bound for the fidelity of the shared state, when all parties are honest, that depends on the pass probability of the test  $P(\rho)$ . We will specifically prove the following theorem:

**Theorem 1** (Honest Case). *Let  $\rho$  be the state shared between  $n$  parties. If  $F(\rho, |G_0^n\rangle) := \langle G_0^n | \rho | G_0^n \rangle$ , where  $|G_0^n\rangle$  is an  $n$ -qubit GHZ state, then  $F(\rho) \geq 2P(\rho) - 1$ .*

Let us define a test in order to verify a ‘rotated’ GHZ state, namely  $|G_\Theta^n\rangle = 1/\sqrt{2}(|0\rangle^{\otimes n} + e^{-i\Theta}|1\rangle^{\otimes n})$ , where  $\Theta \in [0, 2\pi)$ . Here, the sum of the angles of the parties has to comply with the condition:  $\sum_{j=1}^n \theta_j - \Theta \equiv 0 \pmod{\pi}$ . The test that we are interested in is the following:

$$\bigoplus_{j=1}^n Y_j = \frac{\sum_{j=1}^n \theta_j - \Theta}{\pi} \pmod{2} \quad (2)$$

Let  $\{P_\Theta^n, I - P_\Theta^n\}$  be the POVM that corresponds to the above test. We will prove by induction that:

$$P_\Theta^n = |G_\Theta^n\rangle\langle G_\Theta^n| + \frac{1}{2}I_n^\Theta \quad (3)$$

where  $I_n^\Theta$  is the projection on the space orthonormal to  $|G_\Theta^n\rangle$  and  $|G_{\Theta+\pi}^n\rangle$ .

For  $n = 1$  we have that  $P_\Theta^1 = |G_\Theta^1\rangle\langle G_\Theta^1|$  so the statement holds. We assume it is true for  $n$  and we show the statement for  $n + 1$ .

Let  $\{P_\Theta^{n+1}(\theta_1), I - P_\Theta^{n+1}(\theta_1)\}$  be the POVM that corresponds to the test for a given angle  $\theta_1$ . There are two cases:

1. Party 1 outputs  $Y_1 = 0$ . Then, the following equality should hold:

$$\bigoplus_{j=2}^{n+1} Y_j = \frac{\sum_{j=2}^{n+1} \theta_j - (\Theta - \theta_1)}{\pi} \pmod{2} \quad (4)$$

2. Party 1 outputs  $Y_1 = 1$ . Then, the following equality should hold:

$$\bigoplus_{j=2}^{n+1} Y_j = \frac{\sum_{j=2}^{n+1} \theta_j - (\Theta - \theta_1 + \pi)}{\pi} \pmod{2} \quad (5)$$

Let  $\Theta' \equiv \Theta - \theta_1 \pmod{2\pi}$ . It is evident that the first outcome of the test is equivalent to  $P_{\Theta'}^n$  and the second to  $I - P_{\Theta'}^n$ . For any given  $\theta_1$ , we have:

$$\begin{aligned} P_\Theta^{n+1}(\theta_1) &= |G_{\theta_1}^1\rangle\langle G_{\theta_1}^1| \otimes P_{\Theta'}^n + |G_{\theta_1+\pi}^1\rangle\langle G_{\theta_1+\pi}^1| \otimes (I - P_{\Theta'}^n) \\ &= |G_{\theta_1}^1\rangle\langle G_{\theta_1}^1| \otimes |G_{\Theta'}^n\rangle\langle G_{\Theta'}^n| + |G_{\theta_1+\pi}^1\rangle\langle G_{\theta_1+\pi}^1| \otimes |G_{\Theta'+\pi}^n\rangle\langle G_{\Theta'+\pi}^n| \\ &\quad + \frac{1}{2}(|G_{\theta_1}^1\rangle\langle G_{\theta_1}^1| + |G_{\theta_1+\pi}^1\rangle\langle G_{\theta_1+\pi}^1|) \otimes I_n^{\Theta'} \\ &= |G_\Theta^{n+1}\rangle\langle G_\Theta^{n+1}| + |\Phi_{\theta_1}\rangle\langle \Phi_{\theta_1}| + \frac{1}{2}I_1 \otimes I_n^{\Theta'} \end{aligned} \quad (6)$$

where we define:

$$|\Phi_a\rangle = \frac{1}{\sqrt{2}}(|G_a^1\rangle|G_{\Theta-a}^n\rangle - |G_{a+\pi}^1\rangle|G_{\Theta-a+\pi}^n\rangle) \quad (7)$$

It is straightforward to verify that:

$$I_{n+1}^\Theta = |\Phi_{\theta_1}\rangle\langle\Phi_{\theta_1}| + |\Phi_{\theta_1+\frac{\pi}{2}}\rangle\langle\Phi_{\theta_1+\frac{\pi}{2}}| + I_1 \otimes I_n^{\Theta'} \quad (8)$$

where as before  $I_{n+1}^\Theta$  is the projection on the space orthonormal to  $|G_\Theta^{n+1}\rangle$  and  $|G_{\Theta+\pi}^{n+1}\rangle$ . Since angle  $\theta_1$  is chosen uniformly at random in  $[0, \pi)$ , we have that:

$$\begin{aligned} P_\Theta^{n+1} &= \frac{1}{\pi} \int_0^\pi P_\Theta^{n+1}(\theta_1) d\theta_1 \\ &= \frac{1}{\pi} \int_0^{\pi/2} [P_\Theta^{n+1}(\theta_1) + P_\Theta^{n+1}(\theta_1 + \frac{\pi}{2})] d\theta_1 \\ &= |G_\Theta^{n+1}\rangle\langle G_\Theta^{n+1}| + \frac{1}{2} I_{n+1}^\Theta \end{aligned} \quad (9)$$

For  $\Theta = 0 \pmod{2\pi}$ , we can easily infer the basic argument of the proof, that the test is equivalent to performing the POVM  $\{P_0^n, I - P_0^n\}$ . We can therefore express any state  $\rho$  with fidelity  $F(\rho)$  to the GHZ state as  $\rho = F(\rho)|G_0^n\rangle\langle G_0^n| + (1 - F(\rho))\chi$ , where  $\chi$  is a  $2^n \times 2^n$  density matrix with zero in the place of  $|G_0^n\rangle\langle G_0^n|$ . We then have  $P(\rho) = \text{Tr}(P_0^n \rho) \leq \frac{1}{2} + \frac{F(\rho)}{2}$ .

### Security in the Dishonest Model

**Figures of merit for the dishonest case.** Without loss of generality, the source generates a state  $\sum_r p_r |r\rangle\langle r| \otimes |\Psi_r\rangle\langle\Psi_r|_{\mathcal{HDE}}$  where  $r$  corresponds to some classical information controlled by the dishonest players, and  $\mathcal{HDE}$  are respectively the Hilbert space of the honest parties, the dishonest parties and the external environment, which no parties can control.

Here we prove a lower bound for the fidelity of the shared state, when the  $n - k$  parties are dishonest and there are no loss in the system. Since we consider that the dishonest parties can collaborate between themselves and with the source, any security statement should consider that they can apply any operation  $U_r$  (possibly depending on  $r$ ) to their part of the state that works to their advantage. More specifically, we prove the following theorem:

**Theorem 2 (Dishonest Case).** *Let  $\rho = \sum_{r=1}^R p_r |r\rangle\langle r| \otimes \rho_r$  be the state shared between  $n$  parties in the space  $\mathcal{HD}$ . If  $F'(\rho) := \sum_r p_r \max_{U_{n-k}^r} F((\mathbb{I}_k \otimes U_{n-k}^r) \rho_r (\mathbb{I}_k \otimes (U_{n-k}^r)^\dagger), |G_0^n\rangle\langle G_0^n|)$ , where  $U_{n-k}^r$  are operators on the space of the dishonest parties, then  $F'(\rho) \geq 4P(\rho) - 3$ .*

*Proof.*

*Case 1 : Pure state.* We first consider the case without classical information  $r$  and without environment, i.e. where  $\rho$  is a pure state  $|\Psi\rangle\langle\Psi|_{\mathcal{HD}}$ . We write

$$|\Psi\rangle = |G_\theta^k\rangle|\Psi_\theta\rangle + |G_{\pi+\theta}^k\rangle|\Psi_{\pi+\theta}\rangle + |\chi\rangle \quad (10)$$

where  $\theta = \sum_{j \in H} \theta_j \pmod{\pi}$  is the honest angle,  $H$  is the set of the honest parties and  $|G_\alpha^k\rangle = 1/\sqrt{2}(|0\rangle^{\otimes k} + e^{i\alpha}|1\rangle^{\otimes k})$  for any angle  $\alpha$ . Note that the component of the honest parties in  $|\chi\rangle$  is orthogonal to both  $|G_\theta^k\rangle$  and  $|G_{\pi+\theta}^k\rangle$ .

The dishonest parties want to know in which of the two states  $|G_\theta^k\rangle$  and  $|G_{\pi+\theta}^k\rangle$  the state the honest parties share will collapse into after the measurement, and by consequence what will be the honest output  $Y_H = \bigoplus_{i \in H} Y_i$ . They will perform a Helstrom measurement on their share in order to distinguish between  $|\Psi_\theta\rangle$  and  $|\Psi_{\pi+\theta}\rangle$ . This measurement is optimal and gives the following bound:

$$\Pr[\text{guess } Y_H | \theta] = \frac{1}{2} + \frac{1}{2} \left\| |\Psi_\theta\rangle\langle\Psi_\theta| - |\Psi_{\pi+\theta}\rangle\langle\Psi_{\pi+\theta}| \right\| \quad (11)$$

To calculate the above norm, we make use of a known property, that the trace norm of a Hermitian matrix is equal to the sum of the absolute values of its eigenvalues. After some simple calculations we can verify that the above probability is equal to:

$$\begin{aligned} \Pr[\text{guess } Y_H|\theta] &= \frac{1}{2} + \frac{1}{2} \sqrt{(\|\Psi_\theta\|^2 + \|\Psi_{\theta+\pi}\|^2)^2 - 4|\langle\Psi_\theta|\Psi_{\theta+\pi}\rangle|^2} \\ &\leq \frac{1}{2} + \frac{1}{2} \left( \frac{(\|\Psi_\theta\|^2 + \|\Psi_{\theta+\pi}\|^2)^2 - 4|\langle\Psi_\theta|\Psi_{\theta+\pi}\rangle|^2 + 1}{2} \right) \\ &= \frac{3}{4} + \frac{1}{4} \left( (\|\Psi_\theta\|^2 + \|\Psi_{\theta+\pi}\|^2)^2 - 4|\langle\Psi_\theta|\Psi_{\theta+\pi}\rangle|^2 \right) \end{aligned} \quad (12)$$

We now perform a Schmidt decomposition of  $|G_\theta^k\rangle|\Psi_\theta\rangle + |G_{\theta+\pi}^k\rangle|\Psi_{\theta+\pi}\rangle$ :

$$|G_\theta^k\rangle|\Psi_\theta\rangle + |G_{\theta+\pi}^k\rangle|\Psi_{\theta+\pi}\rangle = |A_\theta^0\rangle|B_\theta^0\rangle + |A_\theta^1\rangle|B_\theta^1\rangle \quad (13)$$

where  $\langle A_\theta^0|A_\theta^1\rangle = \langle B_\theta^0|B_\theta^1\rangle = 0$ . We use the following normalization:  $\|A_\theta^0\|^2 = \|A_\theta^1\|^2 = 1$ ,  $\|B_\theta^0\|^2 = p_\theta$ ,  $\|B_\theta^1\|^2 = q_\theta$ . There exist  $z_0, z_1 \in \mathbb{C}$  such that:

$$|A_\theta^0\rangle = z_0 |G_\theta^k\rangle + z_1 |G_{\theta+\pi}^k\rangle \quad \text{and} \quad |A_\theta^1\rangle = z_1^* |G_\theta^k\rangle - z_0^* |G_{\theta+\pi}^k\rangle \quad (14)$$

where  $|z_0|^2 + |z_1|^2 = 1$ , which gives us:

$$\begin{aligned} |A_\theta^0\rangle|B_\theta^0\rangle + |A_\theta^1\rangle|B_\theta^1\rangle &= (z_0 |G_\theta^k\rangle + z_1 |G_{\theta+\pi}^k\rangle)|B_\theta^0\rangle + (z_1^* |G_\theta^k\rangle - z_0^* |G_{\theta+\pi}^k\rangle)|B_\theta^1\rangle \\ &= |G_\theta^k\rangle(z_0 |B_\theta^0\rangle + z_1^* |B_\theta^1\rangle) + |G_{\theta+\pi}^k\rangle(z_1 |B_\theta^0\rangle - z_0^* |B_\theta^1\rangle) \end{aligned} \quad (15)$$

and from Eq. (13) we have:

$$\begin{aligned} |\Psi_\theta\rangle &= z_0 |B_\theta^0\rangle + z_1^* |B_\theta^1\rangle \\ |\Psi_{\theta+\pi}\rangle &= z_1 |B_\theta^0\rangle - z_0^* |B_\theta^1\rangle \end{aligned} \quad (16)$$

Since  $|A_\theta^0\rangle$  and  $|A_\theta^1\rangle$  are on the same subspace as  $|G_\theta^k\rangle$  and  $|G_{\theta+\pi}^k\rangle$ , there exist  $x \in \mathbb{R}, y \in \mathbb{C}$  such that:

$$|A_\theta^0\rangle = x|0^k\rangle + y|1^k\rangle \quad \text{and} \quad |A_\theta^1\rangle = y^*|0^k\rangle - x|1^k\rangle \quad (17)$$

where  $x^2 + |y|^2 = 1$  (we can assume that  $x \in \mathbb{R}$  up to a global phase on  $|A_0\rangle$  and  $|A_1\rangle$ ). Then:

$$|z_0|^2 = |\langle A_\theta^0|G_\theta^k\rangle|^2 = \frac{1}{2}|x + ye^{i\theta}|^2 \quad (18)$$

and since  $y \in \mathbb{C}$ , we rewrite  $y = |y|e^{i\alpha}$  and get:

$$|z_0|^2 = \frac{1}{2}|x + |y|e^{i\theta+\alpha}|^2 = \frac{1}{2}(1 + 2x|y|\cos(\theta + \alpha)) \quad (19)$$

Using  $|z_0|^2 + |z_1|^2 = 1$ , we have  $|z_1|^2 = \frac{1}{2}(1 - 2x|y|\cos(\theta + \alpha))$ . Also, from  $x^2, |y|^2 \geq 0$  and  $x^2 + |y|^2 = 1$ , we have that  $x^2|y|^2 \leq 1/4$ . This gives us:

$$\begin{aligned} |\langle\Psi_\theta|\Psi_{\theta+\pi}\rangle|^2 &= (p_\theta - q_\theta)^2|z_0|^2|z_1|^2 = (p_\theta - q_\theta)^2\frac{1}{4}(1 - 4x^2|y|^2\cos^2(\theta + \alpha)) \\ &\geq (p_\theta - q_\theta)^2\frac{1}{4}(1 - \cos^2(\theta + \alpha)) = (p_\theta - q_\theta)^2\frac{1}{4}\sin^2(\theta + \alpha) \end{aligned} \quad (20)$$

We then revisit Eq. (12):

$$\Pr[\text{guess } Y_H|\theta] \leq \frac{3}{4} + \frac{1}{4}((p_\theta + q_\theta)^2 - (p_\theta - q_\theta)^2\sin^2(\theta + \alpha)) \quad (21)$$

Now, let us consider the optimal local operation that the dishonest parties can perform on their state, in order to maximize their cheating probability. If the reduced density matrices of the honest parties of the ideal state  $|G_0^n\rangle$  and the state  $\rho$  are  $\sigma_H$  and  $\rho_H$  respectively, it holds that there exists a local operation  $R$  on the dishonest state that maximizes the fidelity:

$$F'(\rho) = F((I \otimes R)|\Psi\rangle, |G_0^n\rangle) = F(\sigma_H, \rho_H) \quad (22)$$

Let us decompose  $|G_0^n\rangle$  in the same orthonormal bases for the honest parties, as we did for  $|\Psi\rangle$ . We have  $|G_0^n\rangle = |A_\theta^0\rangle|C^0\rangle + |A_\theta^1\rangle|C^1\rangle$ . Then:

$$\sigma_H = \frac{1}{2}(|A_\theta^0\rangle\langle A_\theta^0| + |A_\theta^1\rangle\langle A_\theta^1|) \quad (23)$$

$$\rho_H = p_\theta|A_\theta^0\rangle\langle A_\theta^0| + q_\theta|A_\theta^1\rangle\langle A_\theta^1| + \text{Tr}_{n-k}|\chi\rangle\langle\chi| \quad (24)$$

and we can express fidelity  $F'(\rho) = \text{Tr}[\sqrt{\sqrt{\rho_H}\sigma_H\sqrt{\rho_H}}]^2$ , which gives:

$$\begin{aligned} F'(\rho) &= \frac{1}{2}(\sqrt{p_\theta} + \sqrt{q_\theta})^2 = \frac{p_\theta + q_\theta}{2} + \sqrt{p_\theta q_\theta} \\ &\geq \frac{(p_\theta + q_\theta)^2}{2} + 2p_\theta q_\theta = (p_\theta + q_\theta)^2 - \frac{(p_\theta - q_\theta)^2}{2} \end{aligned} \quad (25)$$

because for all non-negative  $p$  and  $q$  such that  $p + q \leq 1$ , it holds that  $p + q \geq (p + q)^2$  for  $p + q \leq 1$  and also that  $\sqrt{pq} \geq 2pq$ . Let us note here that whatever decomposition we do to the state  $|\Psi\rangle$ , the sum  $(p_\theta + q_\theta)$  is a constant that always equals  $\|\Psi_\theta\rangle\|^2 + \|\Psi_{\theta+\pi}\rangle\|^2$ . It follows that  $(p_\theta - q_\theta)^2$  is lower bounded by the constant  $2((p_\theta + q_\theta)^2 - F'(\rho))$ . Since  $\theta$  is chosen uniformly at random, we have that:

$$P(\rho) = \frac{1}{\pi} \int_0^\pi \text{Pr}[\text{guess } Y_H|\theta] \quad (26)$$

$$\leq \frac{3}{4} + \frac{1}{4} \left( (p_\theta + q_\theta)^2 - \frac{1}{\pi} \int_0^\pi (p_\theta - q_\theta)^2 \sin^2(\theta + \alpha) d\theta \right) \quad (27)$$

$$\leq \frac{3}{4} + \frac{1}{4} \left( (p_\theta + q_\theta)^2 + F'(\rho) - (p_\theta + q_\theta)^2 \right) \quad (28)$$

$$\leq \frac{3}{4} + \frac{1}{4} F'(\rho) \quad (29)$$

*Case 2 : No classical information, mixed state.* We consider the case where  $\rho = \sum_j q_j |\Psi_j\rangle\langle\Psi_j|_{\mathcal{HD}}$ . Since the two functions  $P(\cdot)$  and  $F(\cdot)$  are linear, we can write

$$P(\rho) = \sum_j q_j P(|\Psi_j\rangle\langle\Psi_j|) \leq \frac{3}{4} + \frac{1}{4} \sum_j q_j F'(|\Psi_j\rangle\langle\Psi_j|) = \frac{3}{4} + \frac{1}{4} F'(\rho) \quad (30)$$

*Case 3 : General Case.* We write  $\rho = \sum_{r=1}^R p_r |r\rangle\langle r| \otimes \rho_r$ . We then write

$$P(\rho) = \sum_r p_r P(\rho_r) = \frac{3}{4} + \frac{1}{4} \sum_r p_r (F(\rho_r)) \quad (31)$$

$$= \frac{3}{4} + \frac{1}{4} \sum_r p_r \max_{U_{n-k}^r} F((\mathbb{I}_k \otimes U_{n-k}^r) \rho_r (\mathbb{I}_k \otimes (U_{n-k}^r)^\dagger), |G_0^n\rangle) \quad (32)$$

□

**Corollary 1.** Let  $\rho$  be the state shared between  $n$  parties. If  $F'(\rho) := \max_U F((\mathbb{I}_k \otimes U_{n-k}) \rho (\mathbb{I}_k \otimes U_{n-k}), |G_0^n\rangle) = \frac{1}{2}$ , where  $U$  is an operator on the space of the dishonest parties, then

1. if the parties run the  $\theta$ -protocol,  $P(\rho|\theta\text{-protocol}) \leq \frac{1}{2} + \frac{1}{\pi}$ .
2. if the parties run the  $XY$ -protocol,  $P(\rho|XY\text{-protocol}) \leq \cos^2(\frac{\pi}{8})$ .

*Proof.* We will first show the upper bound of the pass probability for the  $\theta$ -protocol and then examine the special case where the honest angle  $\theta$  is either equal to 0 or  $\pi/2$ . Following the derivations of Eq. (12) and Eq. (21) we have

$$\begin{aligned}\Pr[\text{guess } Y_H|\theta] &= \frac{1}{2} + \frac{1}{2} \sqrt{(\|\Psi_\theta\|^2 + \|\Psi_{\theta+\pi}\|^2)^2 - 4|\langle\Psi_\theta|\Psi_{\theta+\pi}\rangle|^2} \\ &\leq \frac{1}{2} + \frac{1}{2} \sqrt{(p_\theta + q_\theta)^2 - (p_\theta - q_\theta)^2 \sin^2(\theta + \alpha)}\end{aligned}\quad (33)$$

We know that  $S = p_\theta + q_\theta$  is a constant, independent of  $\theta$ . From Eq. (25) and the fact that  $F'(\rho) = \frac{1}{2}$ , we have that  $2\sqrt{p_\theta q_\theta} = 1 - S$ . We can easily infer:

$$(p_\theta - q_\theta)^2 = S^2 - 4p_\theta q_\theta = 2S - 1 \quad (34)$$

Eq. (33) then becomes:

$$\Pr[\text{guess } Y_H|\theta] \leq \frac{1}{2} + \frac{1}{2} \sqrt{S^2 - (2S - 1) \sin^2(\theta + \alpha)} \quad (35)$$

It also holds that  $F'(\rho) \leq S$  which implies  $S \geq \frac{1}{2}$ . When  $S \in [1/2, 1]$ , we can analytically show that  $P[\rho|\theta\text{-protocol}]$  is maximal for  $S = 1$ . This gives

$$P[\rho|\theta\text{-protocol}] \leq \frac{1}{\pi} \int_0^\pi \frac{1}{2} + \frac{1}{2} \sqrt{1 - \sin^2(\theta + \alpha)} d\theta = \frac{1}{2} + \frac{1}{\pi} \approx 0.818. \quad (36)$$

Now if the parties are running the  $XY$ -protocol, then instead of integrating from 0 to  $\pi$ , we just need to add the cases where  $\theta = 0$  and  $\theta = \pi/2$ . We have:

$$P[\rho|XY\text{-protocol}] = \frac{1}{2} [\Pr[\text{guess } Y_H|0] + \Pr[\text{guess } Y_H|\frac{\pi}{2}]] \quad (37)$$

$$\leq \frac{1}{2} + \frac{1}{4} [\cos^2(\alpha) - \sin^2(\alpha)] \quad (38)$$

Since  $\alpha$  is a characteristic of the state, and can therefore be chosen by the source, the above probability is maximized for  $\alpha = -\pi/4$ , and is equal to  $\cos^2(\pi/8) \approx 0.854$ .

□

### Loss

If the Verifier is willing to accept an individual loss rate  $\lambda$ , then a cheating party can profit from declaring ‘loss’ in order to increase the probability of passing the test. We are interested to see how the two protocols behave in the presence of loss. We concentrate on checking for genuine multipartite entanglement. Since the dishonest parties have full control of the source, and in particular their part (including purification), we treat the dishonest parties as a single system. That is, we say that a source state  $|\psi\rangle_{H,D}$  is genuinely multipartite entangled if it is entangled across all bipartite cuts where  $D$  is treated as a single party (that is all  $D$  systems are on one side of the bipartition).

Looking only at GME in this way greatly simplifies the analysis. We now wish to bound the probability of passing the test for states which are not GME, that is, there exists a partition such that  $|\psi\rangle_{H,D}$  is separable. To bound this take all the honest players which are on  $D$ ’s side of this partition, and imagine the dishonest party has control of them too, *i.e.* we have a bigger  $D$  including these (this cannot but help the dishonest party pass the test). We thus concentrate on product states of the form  $|H\rangle_H \otimes |D\rangle_D$ .

**The  $\theta$ -protocol.** Let  $|H\rangle = \alpha|0\rangle^{\otimes k} + e^{i\theta'}\beta|1\rangle^{\otimes k} + \gamma|X\rangle$  the state shared by the honest players with  $|X\rangle$  orthogonal to both  $|0\rangle^{\otimes k}$  and  $|1\rangle^{\otimes k}$  and  $\alpha, \beta \in \mathbb{R}^+$ . For a fixed  $\theta$  and using the characterization of our test, the honest players will output  $Y_H = 0$  with probability

$$\Pr[Y_H = 0|\theta] = \frac{|\gamma|^2}{2} + \left| \frac{\alpha}{\sqrt{2}} + \frac{\beta}{\sqrt{2}} e^{i(\theta' - \theta)} \right|^2 = \frac{1}{2} + \alpha\beta \cos(\theta' - \theta) \quad (39)$$



The dishonest parties want to guess  $Y_H$ . They will guess  $Y_H = 0$  when  $\cos(\theta' - \theta) \geq 0$  and  $Y_H = 1$  otherwise, and they will succeed with probability  $\frac{1}{2} + \alpha\beta|\cos(\theta' - \theta)|$ . This probability is maximized for  $\alpha, \beta = \frac{1}{\sqrt{2}}$ . Without any loss, the dishonest players succeed with probability:

$$\frac{1}{\pi} \left( \int_0^\pi \frac{1}{2} + \frac{1}{2} |\cos(\theta' - \theta)| d\theta \right) = \frac{2}{\pi} \int_{\theta'}^{\theta' + \pi/2} \cos^2\left(\frac{\theta}{2}\right) d\theta \quad (40)$$

In the case where there is loss, the cheating players can post-select on a  $\lambda$  fraction of the angles. This is the only thing they can do since their state  $|D\rangle$  is unentangled with  $|H\rangle$ . The worst angles are the ones close to  $\pi/2 + \theta'$ . In that case, when the state is tested, the cheating players pass the test with probability:

$$P(\lambda) = \frac{2}{\pi(1-\lambda)} \int_{\theta'}^{\theta' + \pi(1-\lambda)/2} \cos^2\left(\frac{\theta}{2}\right) d\theta = \frac{2}{\pi(1-\lambda)} \int_0^{\pi(1-\lambda)/2} \cos^2\left(\frac{\theta}{2}\right) d\theta \quad (41)$$

**The XY-protocol.** Analyzing this protocol is done in a similar way as before. We start from  $|H\rangle = \alpha|0\rangle^{\otimes k} + e^{i\theta'}\beta|1\rangle^{\otimes k} + \gamma|X\rangle$  with  $\alpha, \beta \in \mathbb{R}^+$ .

- The honest parties receive an even number of Pauli  $Y$  measurement requests: this corresponds to them performing a  $\theta$ -test with  $\theta = 0$ . This means that the honest players output  $Y_H = 0$  with probability  $\frac{1}{2} + \alpha\beta\cos(\theta')$ . The optimal dishonest strategy is to guess  $Y_H = 0$  when  $\cos(\theta') \geq 0$ . Otherwise, they guess  $Y_H = 1$ . This overall strategy will succeed with probability  $\frac{1}{2} + \alpha\beta|\cos(\theta')|$ . Notice that this is maximized for  $\alpha, \beta = \frac{1}{\sqrt{2}}$  which gives  $\Pr[\text{pass test}|\text{even } Y] = \frac{1}{2} + \frac{|\cos(\theta')|}{2}$ .
- The honest parties receive an odd number of Pauli  $Y$  measurement requests: this corresponds to them performing a  $\theta$ -test with  $\theta = \pi/2$ . Similarly as above, we can show that  $\Pr[\text{pass test}|\text{odd } Y] = \frac{1}{2} + \frac{|\cos(\theta' + \pi/2)|}{2} = \frac{1}{2} + \frac{|\sin(\theta')|}{2}$ .

In the case when there is no loss, the pass probability of state  $|H\rangle$  is maximised for  $\theta' = \pi/4$ , since for both measurement settings of the honest parties, the pass probability is  $\cos^2(\pi/8) \approx 0.854$ . For 50% loss, the pass probability of state  $|H\rangle$  is maximised for  $\theta' = 0$ , since whenever the dishonest party is asked to measure in the Pauli  $Y$  basis, he declares loss, resulting in a pass probability equal to 1. For any amount of loss between these two values, the optimal dishonest strategy is a probabilistic mixture of the two pure strategies:

- With probability  $2\lambda$  the source sets  $\theta' = 0$ , and whenever the dishonest party receives  $Y$ , he declares loss.
- With probability  $1 - 2\lambda$  the source sets  $\theta' = \pi/4$ .

Let  $Q(\lambda)$  be the probability that the dishonest parties pass the test, conditioned on not declaring loss. We have:

$$Q(\lambda) = \frac{1}{1-\lambda} (\lambda \cdot \Pr[\text{pass test}|\theta' = 0, X] + (1-2\lambda) \cdot \Pr[\text{pass test}|\theta' = \pi/4]) \quad (42)$$

$$= \frac{\lambda + (1-2\lambda) \cdot 0.854}{1-\lambda} \quad (43)$$

Supplementary Figure 1 shows the difference in the pass probability for the two tests when the amount of tolerated loss increases. Here,  $Q(\lambda)$  is plotted for the XY-protocol test and  $P(\lambda)$  is plotted for the  $\theta$ -protocol test.

## Supplementary Note 2

### State generation

The generation of photon pairs in our setup is achieved by spontaneous four-wave mixing (SFWM) in fiber sources exploiting birefringent phase-matching [1, 2]. The fibers are strongly birefringent ( $\Delta n = 4 \times 10^{-4}$ ) and microstructured, with the phase-matching generating signal-idler pairs cross-polarization to the pump laser. The waveguide contributions to the dispersion in addition to the birefringence tailor the SFWM to the generation of naturally narrowband spectrally uncorrelated photons when pumped with Ti-Sapphire laser pulses at 726nm. This is achieved at the flat region of the phase-matching curves upon which the idler photons ( $\lambda_i = 871$  nm) are group velocity matched to the pump pulse so that they become spectrally broad ( $\Delta\lambda_i = 2.2$  nm) whilst the signal photons ( $\lambda_s = 623$  nm) are intrinsically narrowband ( $\Delta\lambda_s = 0.3$  nm). This narrowband phase-matching results in a Joint-Spectral Amplitude (JSA) which is highly separable for a wide range of pump bandwidths and thus single photons of high purity can be produced. The pump bandwidth can then be tuned to minimize the effects of deviating from the flat region at 726 nm whilst reducing the self-phase modulation caused by short pulses, to arrive at an optimal pump bandwidth of  $\Delta\lambda_p = 1.7$  nm.

The fiber sources are then positioned in Sagnac-loop configurations in which the pump pulse is set to diagonal polarization and split at a polarizing beam-splitter (PBS), after which it is launched into the fiber in both directions simultaneously. The 90° rotation of the fiber axis between its two facets results in the pump light being strongly suppressed out of the port of the PBS it entered, whilst the generated signal-idler pairs from each facet of the fiber are cross-polarized to the pump that generated them, so exit from the other port to the pump. The pairs generated from each direction traverse the same mode in reverse so on exiting the PBS they coherently share the same spatio-temporal mode and create the state  $\frac{1}{\sqrt{2}}(|H\rangle_s |H\rangle_i + e^{i\theta} |V\rangle_s |V\rangle_i)$  up to some phase  $\theta$ .

The generation of three- and four-photon GHZ states in our setup is then achieved by a parity check, or ‘fusion’, with post-selection [3–6]. Fusion processes of this sort require photons originating from two distinct sources to be indistinguishable in all degrees of freedom, however the fabrication of microstructured fibres can result in small inhomogeneities between fiber samples. To overcome these inhomogeneities one fiber source is temperature tuned so that the spectra of the signal photons match the spectra of the signal photons in the other fiber. This reduces the distinguishability. The spectra of the signal photons from each source were measured for a range of pump bandwidths and Gaussians fitted to determine their central wavelength. The second source was then temperature tuned using a Peltier cooler to 23.7°C (relative to the ambient 17.6°C) to achieve optimal indistinguishability in the spectra (see Supplementary Figure 2). It is useful to note here that despite the inhomogeneous distribution of heat to the fiber, which results in significant broadening of the idler photon, the narrowband phase-matching scheme ensures that the signal photon remains narrowband. However, note there are still small differences between the signal spectra that arise from inhomogeneities in the fibre and these reduce the maximum fidelity achievable.

The generation of the four-photon GHZ state proceeds by overlapping the signal photons from two Bell pair sources at a PBS and post-selecting the event in which one photon is detected at each output port. On the other hand, the three-photon GHZ state requires one of the sources to contribute just a single heralded signal photon in the state  $|D\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$  and post-selecting similarly. This is achieved by pumping the second source in only one direction and rotating the heralded signal photon with a half-wave plate.

Arbitrary local projective measurements are achieved by polarisation rotations using pairs of half- and quarter-wave plates, followed by polarising beam splitters (PBSs) to spatially separate the two eigenstates of polarisation, before collection into 8 silicon avalanche photodiode detectors. Pairs of automated achromatic half- and quarter-wave plates were calibrated to account for the chromatic deviations at signal and idler wavelengths, and numerical methods were used to find wave plate angles to map the input states to the states closest to the ideal projection vectors. Note that due to the chromatic deviations of wave plates, not all rotations can necessarily be achieved, so to allow the Pauli bases and the X-Y equator to be reached, appropriate approximate states were chosen by fiber polarizers for input to the measurement stage.

### Higher-order terms from sources

#### 4-qubit GHZ

The state generated by four-wave mixing in one source in an ‘entangled configuration’ can be written as [7]

$$|\psi\rangle_{s,i} = \mathcal{N}(|0,0\rangle_{s,i} + \alpha(|1_H, 1_H\rangle_{s,i} + |1_V, 1_V\rangle_{s,i}) + \alpha^2(|2_H, 2_H\rangle_{s,i} + |2_V, 2_V\rangle_{s,i} + |1_H 1_V, 1_H 1_V\rangle_{s,i}) + \mathcal{O}(\alpha^3)), \quad (44)$$

where  $\mathcal{N}$  is a normalisation constant,  $|\alpha|^2 = \bar{n}/(\bar{n} + 1)$  is the mean number of signal-idler pairs generated in a pulse and  $|\ell_{H/V}\rangle_k = \frac{1}{\sqrt{\ell!}}(\hat{a}_{H/V,k}^\dagger)^\ell |0\rangle_k$  for mode  $k$ . Taking two sources in the entangled configuration we have the starting state

$$|\psi\rangle_{s_1,i_1,s_2,i_2} = \mathcal{N}(|0,0\rangle_{s_1,i_1} + \alpha(|1_H, 1_H\rangle_{s_1,i_1} + |1_V, 1_V\rangle_{s_1,i_1}) + \alpha^2(|2_H, 2_H\rangle_{s_1,i_1} + |2_V, 2_V\rangle_{s_1,i_1} + |1_H 1_V, 1_H 1_V\rangle_{s_1,i_1}) + \mathcal{O}(\alpha^3)) \otimes (|0,0\rangle_{s_2,i_2} + \alpha(|1_H, 1_H\rangle_{s_2,i_2} + |1_V, 1_V\rangle_{s_2,i_2}) + \alpha^2(|2_H, 2_H\rangle_{s_2,i_2} + |2_V, 2_V\rangle_{s_2,i_2} + |1_H 1_V, 1_H 1_V\rangle_{s_2,i_2}) + \mathcal{O}(\alpha^3)), \quad (45)$$

which gives 35 terms when expanded up to  $\alpha^3$ . Applying the PBS transformations for the fusion:  $\hat{a}_{H,s_1} \rightarrow \hat{a}_{H,s_1}, \hat{a}_{V,s_1} \rightarrow \hat{a}_{V,s_2}, \hat{a}_{H,s_2} \rightarrow \hat{a}_{H,s_2}$  and  $\hat{a}_{V,s_2} \rightarrow \hat{a}_{V,s_1}$ , and taking terms that have at least one photon in each mode we have the state

$$|\psi\rangle = \mathcal{N}(\alpha^2(|1_H, 1_H, 1_H, 1_H\rangle + |1_V, 1_V, 1_V, 1_V\rangle) + \alpha^3(|2_H, 2_H, 1_H, 1_H\rangle + |1_H, 1_H, 2_H, 2_H\rangle + |2_V, 1_V, 1_V, 2_V\rangle + |1_V, 2_V, 2_V, 1_V\rangle + \frac{1}{2}(|1_H 1_V, 1_H, 1_V, 1_H 1_V\rangle + |1_H 1_V, 1_H 1_V, 1_V, 1_V\rangle + |1_H, 1_H 1_V, 1_H 1_V, 1_H\rangle + |1_V, 1_V, 1_H 1_V, 1_H 1_V\rangle)))_{s_1,i_1,s_2,i_2}, \quad (46)$$

where the terms with  $\alpha^2$  lead to the desired GHZ state and higher-order terms with  $\alpha^3$  cause the state to be non-ideal. Here we have not included the possibility of further postselection depending on the measurement basis. For example, in the H/V basis the last 4 terms can be dropped, as two photons in a single mode will lead to both detectors from the polarisation analysis of that mode giving a click. This is not the case for all bases however.

The fidelity of  $|\psi\rangle$  with respect to the ideal GHZ state is  $F = 2\alpha^4/(2\alpha^4 + 5\alpha^6)$ . For the pump power used in our experiment of  $P = 7$  mW in each fibre in each direction we have  $\bar{n} = 0.05$  and therefore  $\alpha = 0.22$ , leading to a fidelity of  $F = 0.89$ . Thus, higher-order emissions up to  $\alpha^3$  reduce the quality of the state, as measured using the fidelity, by 11%. Terms with  $\alpha^4$  are 0.22 times smaller than those with  $\alpha^3$  and will therefore have a contribution of only 1 – 2%. At the pump power used we have a rate of four-folds of 1-2  $s^{-1}$ . An interesting question is whether the higher-order emissions can be used by the dishonest parties to gain an advantage when loss is present. This is a system dependent issue which we leave for future work. However, we note that regardless of this, by using a smaller pump power one can reduce the impact of higher order terms on the fidelity in our setup, although at the expense of the overall four-fold rate. For example, with  $P = 1$  mW one can reduce the impact on the fidelity to only 2%.

### 3-qubit GHZ

The state generated by four-wave mixing in one source in a ‘product configuration’ can be written as [7]

$$|\psi\rangle_{s,i} = \mathcal{N}(|0, 0\rangle_{s,i} + \alpha |1_H, 1_H\rangle_{s,i} + \alpha^2 |2_H, 2_H\rangle_{s,i} + \mathcal{O}(\alpha^3)). \quad (47)$$

Taking one source in the product configuration and the other in the entangled configuration we have the starting state

$$\begin{aligned} |\psi\rangle_{s_1,i_1,s_2,i_2} &= \mathcal{N}(|0, 0\rangle_{s_1,i_1} + \alpha |1_H, 1_H\rangle_{s_1,i_1} + \alpha^2 |2_H, 2_H\rangle_{s_1,i_1} + \mathcal{O}(\alpha^3)) \otimes \\ &\quad (|0, 0\rangle_{s_2,i_2} + \alpha(|1_H, 1_H\rangle_{s_2,i_2} + |1_V, 1_V\rangle_{s_2,i_2}) \\ &\quad + \alpha^2(|2_H, 2_H\rangle_{s_2,i_2} + |2_V, 2_V\rangle_{s_2,i_2} + |1_H 1_V, 1_H 1_V\rangle_{s_2,i_2}) + \mathcal{O}(\alpha^3)). \end{aligned} \quad (48)$$

which gives 20 terms when expanded up to  $\alpha^3$ . Applying the HWP on mode  $s_1$ :  $\hat{a}_{H,s_1} \rightarrow \frac{1}{\sqrt{2}}(\hat{a}_{H,s_1} + \hat{a}_{V,s_1})$ , and the PBS transformations for the fusion:  $\hat{a}_{H,s_1} \rightarrow \hat{a}_{H,s_1}, \hat{a}_{V,s_1} \rightarrow \hat{a}_{V,s_2}, \hat{a}_{H,s_2} \rightarrow \hat{a}_{H,s_2}$  and  $\hat{a}_{V,s_2} \rightarrow \hat{a}_{V,s_1}$ , and taking terms that have at least one photon in each mode we have the state (conditioned on a detection of one or more photons in mode  $i_1$ )

$$\begin{aligned} |\psi\rangle &= \mathcal{N}[\frac{\alpha^2}{\sqrt{2}}(|1_H, 1_H, 1_H\rangle + |1_V, 1_V, 1_V\rangle) + \frac{\alpha^3}{\sqrt{2}}(|1_H, 2_H, 2_H\rangle + |2_V, 1_V, 2_V\rangle \\ &\quad + \frac{1}{2}|1_H 1_V, 1_H, 1_H 1_V\rangle + \frac{1}{2}|1_V, 1_H 1_V, 1_H 1_V\rangle + \frac{1}{\sqrt{2}}|2_H, 1_H, 1_H\rangle + \frac{1}{\sqrt{2}}|1_V, 2_V, 1_V\rangle \\ &\quad + |1_H 1_V, 1_V, 1_V\rangle + |1_H, 1_H 1_V, 1_H\rangle)]_{s_1,s_2,i_2}, \end{aligned} \quad (49)$$

where the terms with  $\alpha^2$  lead to the desired GHZ state and higher-order terms with  $\alpha^3$  cause the state to be non-ideal. Here we have again not included the possibility of further postselection depending on the measurement basis.

The fidelity of  $|\psi\rangle$  with respect to the ideal GHZ state is  $F = \alpha^4/(\alpha^4 + \frac{11}{4}\alpha^6)$ . For the pump power used in our experiment of  $P = 7$  mW in each fibre in each direction (with the source in the product configuration only pumped in one direction) we have  $\bar{n} = 0.05$  and therefore  $\alpha = 0.22$ , leading to a fidelity of  $F = 0.88$ . Thus, higher-order emissions up to  $\alpha^3$  reduce the quality of the state, as measured using the fidelity, by 12%. Terms with  $\alpha^4$  are 0.22 times smaller than those with  $\alpha^3$  and will therefore have a contribution of only 1 – 2%. Again, for a low pump power of  $P = 1$  mW one can reduce the impact of the higher order terms on the fidelity to 2%.

---

\* Electronic address: annapappa@gmail.com

† Electronic address: markstame@gmail.com

- [1] M. Halder, J. Fulconis, B. Cerny, A. Clark, C. Xiong, W. J. Wadsworth and J. G. Rarity, Nonclassical 2-photon interference with separate intrinsically narrowband fibre sources, *Optics Express* **17**, 4670-4676 (2009).
- [2] A. Clark, B. Bell, J. Fulconis, M. M. Halder, B. Cerny, O. Alibart, C. Xiong, W. J. Wadsworth and J. G. Rarity, Intrinsically narrowband pair photon generation in microstructured fibres, *New J. Phys.* **13**, 065009 (2011).
- [3] T. B. Pittman, B. C. Jacobs and J. D. Franson, Probabilistic quantum logic operations using polarizing beam splitters, *Phys. Rev. A* **64**, 062311 (2001).

- [4] J.-W. Pan, C. Simon, C. Brukner and A. Zeilinger, Entanglement purification for quantum communication, *Nature* **410**, 1067 (2001).
- [5] J.-W. Pan, S. Gasparoni, R. Ursin, G. Weihs and A. Zeilinger, Experimental entanglement purification of arbitrary unknown states, *Nature* **423**, 417 (2003).
- [6] B. Bell, A. Clark, M. S. Tame, M. Halder, J. Fulconis, W. Wadsworth and J. Rarity, Experimental characterization of photonic fusion using fiber sources, *New J. Phys.* **14**, 023021 (2012).
- [7] J. Fulconis, O. Alibart, W. J. Wadsworth and J. G. Rarity, Quantum interference with photon pairs using two micro-structured fibres, *New J. Phys.* **9**, 276 (2007).